BioPass
Manual do Usuário

Atlas Schindler

Índice

1. Introdução ... 1
2. Equipamentos ... 2
   2.1. Unidade Gerenciadora ... 2
   2.2. Unidade Cadastradora ... 2
   2.3. Unidade de Leitura Biométrica ... 2
3. Cuidados com o equipamento ... 3
4. Funcionamento do sistema ... 4
   4.1. Digital de acesso ... 5
   4.2. Digital chave ... 5
   4.3. Digital de segurança ... 5
   4.4. Cartão de acesso - BioPass Sensor ... 5
   4.5. Cartão chave - BioPass Sensor ... 5
5. Programa de controle ... 6
   5.1. Estrutura e menus de comando ... 7
6. Cadastramento ... 8
   6.1. Cadastramento de operadores ... 8
   6.2. Cadastramento de usuários ... 10
   6.2.1. Usuário: Cadastro de Dados Pessoais e Perfil de Acesso ... 11
   6.2.2. Biometria: Cadastro das Digitais e Configurações do Acesso ... 12
   6.2.3. RFID: Cadastro do Cartão e Configurações de Acesso ... 17
7. Possíveis problemas ... 21
8. Gerenciamento ... 22
   8.1. Localizar usuário ... 22
   8.2. Modificar usuário ... 22
   8.3. Análise do usuário ... 22
   8.4. Histórico de eventos ... 23
9. Funções avançadas ... 25
   9.1. Andares liberados pelo usuário ... 25
   9.2. Bloqueio do andar liberado pelo usuário ... 25
   9.3. Andares comuns ... 26
   9.4. Andar X ... 26
   9.5. Capturar imagem ... 26
   9.6. Atualizar Templates ... 28
   9.7. Análise de Consistência ... 29
   9.8. Reinicialização: Resetar ... 30
   9.9. Cópia de Segurança ... 31
   9.10. Status do usuário ... 32
   9.11. Edifício ... 33
   9.12. Habilitar Aviso de Alarme ... 34
   9.13. Mudança de Idioma ... 35
10. Advertência ... 36

1. Introdução

Biometria é um método automatizado de reconhecimento pessoal baseado em características fisiológicas ou comportamentais. O reconhecimento é totalmente pessoal e intransferível.

Não há necessidade de chaves, senhas ou qualquer outro dispositivo que seja necessário trazer consigo. Basta utilizar a impressão digital de qualquer dedo.

A tecnologia de reconhecimento de impressões digitais utilizada no sistema **BioPass** é do tipo capacitivo. Este tipo de tecnologia torna inviável ou dificulta ao extremo as tentativas indevidas de acesso ao sistema.

O sistema **BioPass** possibilita o cadastramento de toda a população de um condomínio: moradores, visitantes e funcionários. Permite a diferenciação entre eles e possibilita a restrição de acesso aos elevadores, inclusive por dias e horários.

Uma das características do sistema é a possibilidade de atribuição de uma 2ª digital, denominada **Digital de Segurança**, que permite ao usuário avisar que se encontra em uma situação de perigo ou ameaça.

Outra característica do sistema é o cadastro de uma 3ª digital, denominada **Digital Chave**, com a finalidade de permitir ao usuário liberar o acesso ao seu andar.

Visando garantir que todos os usuários estejam integrados ao sistema **BioPass**, foi incorporado ao sistema um dispositivo que permite a leitura de cartões do tipo proximidade (**RFID**). Este sistema adicional é denominado **BioPass Sensor**, ampliando o uso do sistema e facilitando a utilização por usuários com dificuldade de cadastramento, utilização por visitantes e prestadores de serviço.

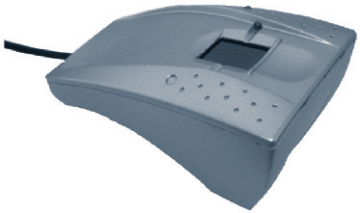
O símbolo indica a presença desta funcionalidade nas unidades leitoras de cabina.

2. Equipamentos

2.1. Unidade Gerenciadora

A Unidade Gerenciadora fica localizada na **portaria** ou em uma **sala de segurança** do condomíno e é responsável pelo gerenciamento do sistema de controle de acesso biométrico.

2.2. Unidade Cadastradora



Dispositivo utilizado para cadastramento das digitais do sistema, fica localizado próximo a Unidade Gerenciadora.

2.3. Unidade de Leitura Biométrica

Dispositivo localizado na cabina do elevador, junto à botoeira, utilizado para controle de acesso aos pavimentos privativos.

3. Cuidados com o equipamento

Proteção do sensor

Pelo fato do sensor biométrico ter o seu circuito eletrônico diretamente em contato com a pele do usuário, certos tipos de cuidados são necessários para garantir a leitura correta, a manutenção e a integridade da célula biométrica.

Siga as seguintes indicações:

- Não arranhe a superfície do sensor com nenhum tipo de objeto duro ou ferramenta.
- Não apoie ou coloque objetos pesados sobre ou próximo ao sensor.
- Não aplique nenhum tipo de ácido ou outros tipos de líquidos agressivos como colas, pastas, pomadas ou substância similar diretamente sobre a superfície do sensor.
- Não utilize esponja de aço para limpeza do sensor.

Limpeza do sensor

Para a limpeza apropriada do sensor, siga as seguintes recomendações:

- Para uma limpeza básica, use pano seco ou levemente umedecido, de algodão ou outro tecido não fibroso para remover a sujeira da superfície do sensor.
- Em casos raros (após longos períodos sem limpeza), partículas mais resistentes podem não ser removidas pelo método acima. Neste caso, utilize produto do tipo limpa-vidros doméstico.
- Após limpar a superfície do sensor com limpa-vidros, finalize com um pano levemente umedecido como indicado acima.

ATENÇÃO

- Não utilize limpa-vidros industriais. Estes produtos contêm substâncias que podem causar danos ao sensor.
- A água e a maioria dos líquidos são eletricamente condutivo e podem causar falhas no funcionamento e até mesmo danos aos componentes. A superfície do sensor é resistente a água por curtos intervalos de tempo.
- Nunca limpe o sensor com qualquer tipo de material áspero.

4. Funcionamento do sistema

Para ter livre acesso e fazer uso dos elevadores, o passageiro deve estar previamente cadastrado no sistema.

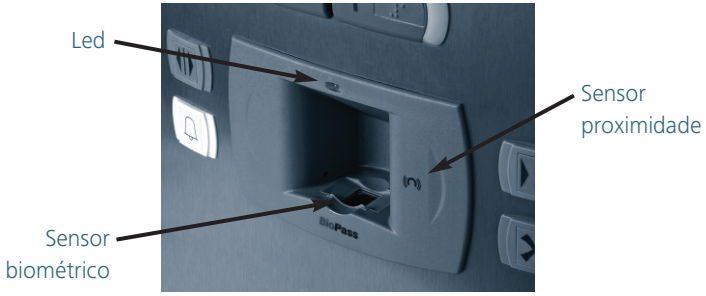
Esse cadastramento deverá ser realizado somente pela(s) pessoa(s) indicada(s) como responsável no condomínio ou, extraordinariamente, pelo pessoal de **Suporte** da Atlas Schindler.

Ao entrar na cabina, coloque a digital cadastrada sobre o sensor biométrico, localizado na botoeira, ou aproxime o cartão, do tipo proximidade (**RFID**), da região demarcada com o símbolo . Imediatamente o sensor reconhecerá sua presença, fazendo com que durante o processo de reconhecimento um led pisque na **cor amarela**.

Se o usuário for reconhecido, o led acenderá na **cor verde** e emitirá um sinal sonoro confirmando o reconhecimento. Neste momento, somente os botões associados aos andares que o usuário está autorizado a acessar serão desbloqueados.

Se o usuário não for reconhecido, o led acendará na **cor vermelha** e emitirá dois sinais sonoros, ficando o usuário impedido de acessar qualquer andar privativo.

Caso não ocorra o reconhecimento de um usuário cadastrado, favor consultar a seção "**Possíveis problemas**".



O sistema **BioPass** permite o cadastramento de até três tipos de digitais que possuem diferentes funções e a associação a um cartão do tipo proximidade (**RFID**) por usuário:

4.1. Digital de acesso

O cadastro da **Digital de Acesso** é necessário para a utilização do elevador, seja de um morador, visitante ou funcionário. Neste cadastro, é realizada a diferenciação entre os usuários, podendo ser restringido o acesso a uma programação predeterminada.

4.2. Digital chave

Existe ainda a opção de cadastrar a 2ª impressão digital, denominada **Digital Chave**. Este recurso permite ao usuário desativar ou reativar, quando necessário, o uso do sistema biométrico para acesso ao seu pavimento. Ou seja, essa digital alterna o sistema com restrição e sem restrição de acesso. A **Digital Chave** libera ou restringe o acesso a um único pavimento, devendo ser preferencialmente o andar de residência do usuário.

4.3. Digital de segurança

O cadastro da 3ª digital define a **Digital de Segurança**. A **Digital de Segurança** (**Templates para alarme**) tem as mesmas funcionalidades da **Digital de Acesso**, com exceção de um atributo especial que faz disparar um alarme silencioso, num local definido pelo cliente, avisando que o usuário encontra-se sob alguma forma de perigo ou ameaça.

4.4. Cartão de acesso - BioPass Sensor

O cartão de acesso, tipo proximidade (RFID), possui todas as funcionalidades da **Digital de Acesso**, podendo ser utilizado por morador, visitante ou funcionário. No cadastro do **Cartão de Acesso**, é realizada a diferenciação entre usuários, podendo ser restringido o acesso a uma programação predeterminada.

4.5. Cartão Chave - BioPass Sensor

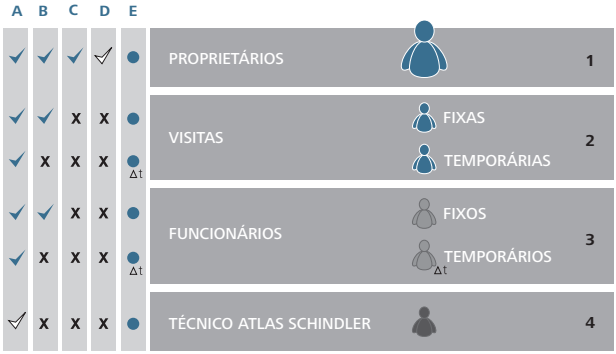
O **Cartão Chave**, tipo proximidade (**RFID chave**), possui todas as funcionalidades da **Digital Chave**, podendo ser utilizado somente por morador.

Nota:

Verifique no capítulo **Cadastramento** o procedimento para cadastrar a **Digital de Acesso**, a **Digital de Segurança**, a **Digital Chave**, o **Cartão de Acesso** e o **Cartão Chave**, ambos tipo proximidade **RFID**.

Os usuários têm diferentes níveis de autorização, conforme abaixo:

A - Digital de Acesso
B - Digital de Segurança
C - Digital-chave
D - Cartão Chave
E - Cartão de Acesso

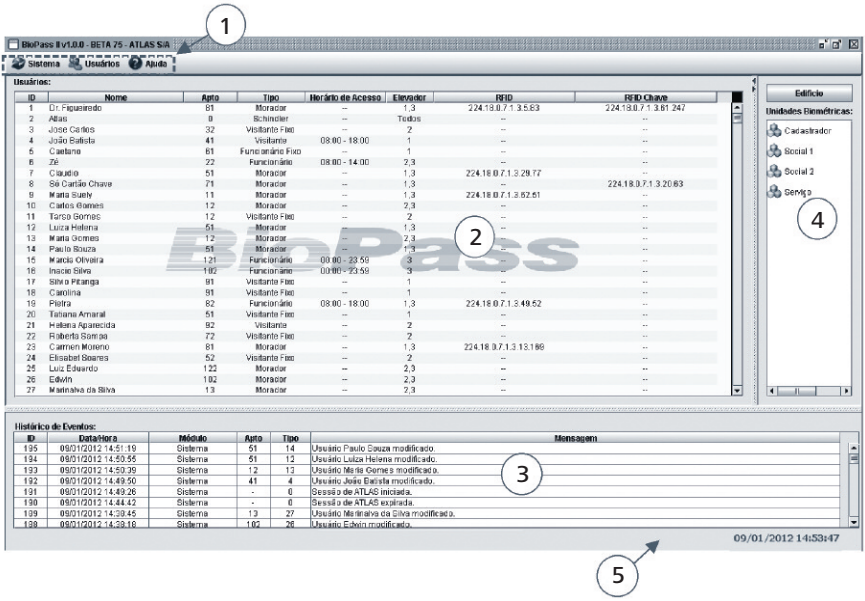


5. Programa de controle

O software de controle, que consiste em uma interface homem-máquina, foi desenvolvido para permitir a interação entre o usuário e o sistema **BioPass Java**. Através dele será possível configurar os dispositivos do sistema, cadastrar e gerenciar o acesso dos usuários, monitorar eventos e status que ocorram durante a sua utilização.

Na figura a seguir, temos uma panorâmica da tela principal do software de controle, composta por cinco campos:

1. Menus (**Sistema**, **usuário** e **ajuda**);
2. Campo de usuários cadastrados;
3. Campo de histórico de eventos (**Log**);
4. Estrutura de andares liberados;
5. Barra de **status**, **data** e **hora**.



5.1. Estrutura e menus de comando

Perfil: **Suporte**

Sistema	Usuário	Ajuda
Logoff*	Cadastrar	Ajuda sobre o BioPass
Identidade	Modificar	Sobre o BioPass
Idioma	Apagar	
Avisos	Localizar CTRL-F	
Unidade biométrica		
Configurar		
Testar conexão		
Capturar imagem		
Atualizar templates		
Apagar templates		
Análise de consistência		
Resetar		
Configurações originais		
Cópia de segurança		
Histórico		
Sair		

Perfil: **Administrador**

Sistema	Localizar	Ajuda
Logoff*	Cadastrar	Ajuda sobre o BioPass
Identidade	Modificar	Sobre o BioPass
Idioma	Apagar	
Avisos	Localizar CTRL-F	
Unidade biométrica		
Configurar		
Testar conexão		
Capturar imagem		
Atualizar templates		
Apagar templates		
Análise de consistência		
Resetar		
Configurações originais		
Cópia de segurança		
Histórico		
Sair		

Perfil: **Porteiro**

Sistema	Localizar	Ajuda
Logoff*	Cadastrar	Ajuda sobre o BioPass
Identidade	Modificar	Sobre o BioPass
Idioma	Apagar	
Avisos	Localizar CTRL-F	
Unidade biométrica		
Cópia de segurança		
Histórico		
Sair		

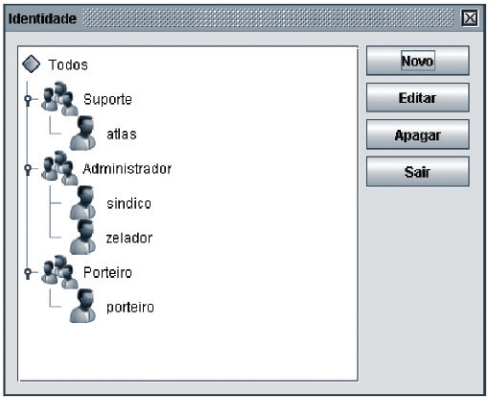
* **Logoff**: comando a ser executado para encerrar a utilização do programa de gerenciamento pelo usuário.

6. Cadastramento

6.1. Cadastramento de operadores

Para que se tenha o acesso ao programa de controle instalado na **Unidade Gerenciadora**, é necessário o cadastramento de um usuário (**Login**) e uma senha de acesso.

Este cadastro poderá ser realizado com 3 níveis diferentes, de forma que cada um tenha funções e autorizações distintas.



Níveis de acesso

Suporte - Nível de acesso total

Trata-se do técnico da Atlas Schindler, o responsável pela total configuração do sistema. É ele quem cria os logins de acesso para **Administradores** e cuida da manutenção, funcionamento e atualizações do sistema **BioPass** .

Administrador - Nível intermediário de autorização

O usuário cadastrado nesse nível de autorização terá as seguinte atribuições:

- Adicionar usuário com login de acesso tipo **Administrador** ou **Porteiro**.
- Cadastrar um novo usuário.
- Apagar usuário cadastrado.
- Mudar as características de um usuário existente. Por exemplo, se for um visitante, ele poderá alterar os dias e horários permitidos ao acesso.

- Associar ou modificar um **Cartão de Acesso** do tipo aproximação (**RFID**) a um usuário.
- Associar ou modificar um **Cartão Chave** do tipo aproximação (**RFID**) a um morador.
- Acrescentar uma impressão digital para um usuário já cadastrado.
- Modificar o status da impressão **Digital de Acesso** para **Digital de Segurança** ou **Digital Chave**.
- Modificar os andares que o usuário (morador, visitante ou funcionário) tem acesso.
- Gerar ou restaurar a **Cópia de Segurança** do sistema.
- Reinicializar as unidades biométricas dos elevadores.
- Exportar dados para emissão de relatórios.
- Atualizar os templates.
- Efetuar a **Análise de Consistência**.

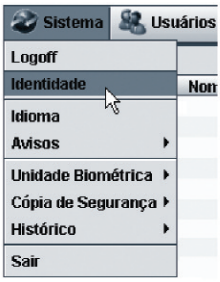
Porteiro - Nível mais restrito de autorização:
O usuário cadastrado com o status de **Porteiro** terá permissão para:
- Alterar sua senha de acesso.
- Listar usuários cadastrados.
- Localizar usuários cadastrados.
- Consultar características de usuários cadastrados.
- Ativar a restrição de acesso a um andar, desativado por um morador (por meio da Digital Chave ou do Cartão Chave), e que esqueceu de reativá-la.

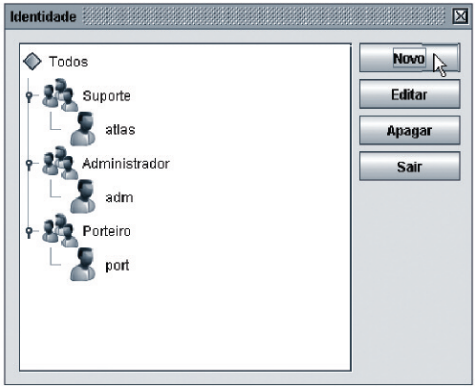
Processo de cadastramento (Identidade)

É possível cadastrar mais de um **Administrador** e **Porteiro** por edifício.

Para criar uma identidade, execute o seguinte procedimento:

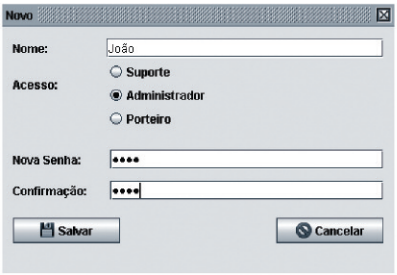
a) No menu "**Sistema**", selecione o item "**Identidade**", clique no botão **Novo** e realize o cadastro, configurando as respectivas limitações de acesso.

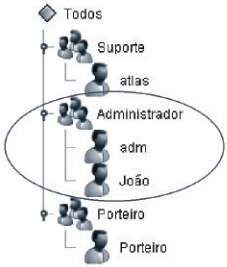




b) Digite o nome do operador, por exemplo: "João".
c) Selecione o perfil de acesso, por exemplo: "**Administrador**".
d) Digite a nova senha, no campo **Nova Senha**.
e) Confirme a nova senha, no campo **Confirmação**.
f) Clique no botão **Salvar**.

Feito isso, o usuário "João" foi cadastrado como **Administrador**.





Notas:
- O perfil **Suporte** tem acesso aos níveis: **Suporte**, **Administrador** e **Porteiro**.
- O perfil **Adminstrador** tem acesso aos níveis: **Administrador** e **Porteiro**.
- O perfil **Porteiro** tem acesso somente ao nível: **Porteiro**.

6.2. Cadastramento de usuários

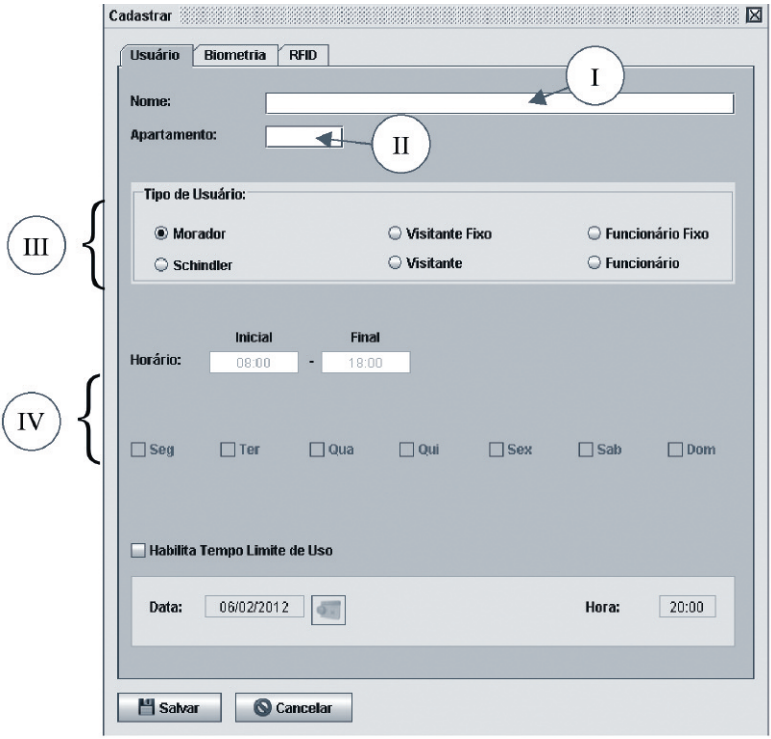
Para o cadastramento, é necessário ter o nível de autorização de **Administrador**. Caso esse nível de autorização não tenha sido cadastrado ainda, verifique o **capítulo 6.1**.

No menu **Usuário** selecione o item **Cadastrar**.

O cadastro do usuário será feito em até três etapas:
- Usuário ➔ Dados Pessoais e Perfil de Acesso.
- Biometria ➔ Cadastro das digitais e configuração de acesso.
- RFID ➔ Cadastro do **Cartão BioPass Sensor** e configuração de acesso.

6.2.1. Usuário: Cadastro de Dados Pessoais e Perfil de Acesso

O início do cadastro ocorre na aba "**Usuário**", onde são inseridos os dados pessoais.



I) Nome

Escreva o nome do morador, funcionário ou visitante a ser cadastrado. Se desejar, utilize este campo também para registrar o número do documento de identidade e/ou alguma outra informação relevante.

II) Apartamento

Preencha com o número do apartamento no qual o usuário terá acesso, ou seja, onde ele mora ou irá visitar.

Nota:

Os campos **Nome** e **Apartamento** são itens obrigatórios.

III) Tipo de Usuários

Selecione a categoria deste registro:

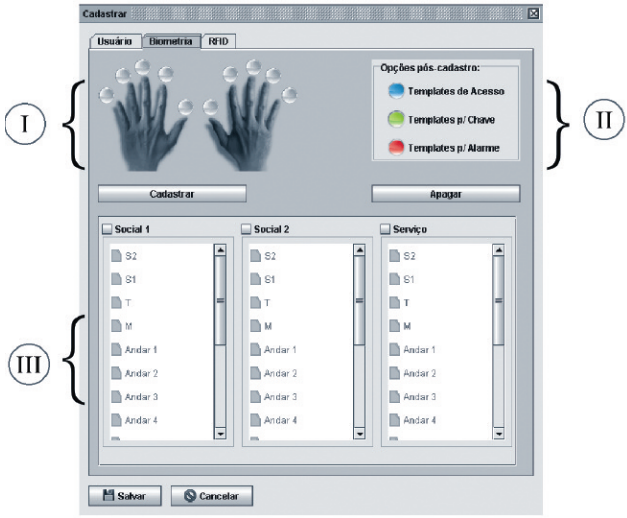
- **Morador:** Usuário que reside no prédio.
- **Visitante Fixo:** Usuário que não reside no prédio, mas possui acesso constante, como: familiares, amigos íntimos etc.
- **Visitante:** Usuário ocasional.
- **Funcionário Fixo:** Empregados do condomínio ou dos condôminos que residam ou não, porém com acesso diário, como: empregados domésticos, zelador, faxineiros etc.
- **Funcionário:** Prestador de serviço sem vínculo com o condomínio ou com os condôminos, como: encanador, pintor, pedreiro etc.
- **Schindler:** Técnico da Atlas Schindler.

IV) Horário e dias da semana

Para **Visitantes** e **Funcionários**, é permitido restringir os dias e horário de acesso. Para isso, selecione os dias da semana e o horário de acesso permitidos para esse usuário.

6.2.2. Biometria: Cadastro das Digitais e Configurações do Acesso

A aba "**Biometria**" é destinada ao cadastro das características biométricas e da configuração do acesso para uso da biometria:



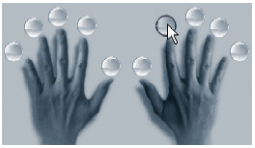
I) Cadastro das digitais
II) Opções pós- cadastro
III) Configuração do Acesso para Biometria

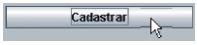
Cada digital deverá ser cadastrada **3 vezes**, obedecendo as instruções abaixo:

I) Cadastro das Digitais

Para cadastrar uma digital, execute o seguinte procedimento:

a) Escolha o dedo e selecione a respectiva **bolinha branca**.



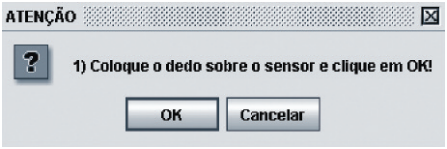
b) Clique no botão **CADASTRAR** ➔ 

c) Posicione corretamente o dedo sobre o sensor biométrico do cadastrador.

ATENÇÃO

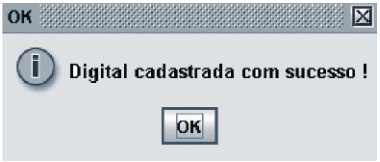
É importante o posicionamento correto do dedo na célula biométrica. A dobra da primeira falange do dedo deve coincidir com o ressalto da **unidade biométrica de cadastramento**, conforme figuras abaixo:

d) Feito isso, clique no botão **OK**.



e) Retire o dedo do cadastrador.

f) Repita esse procedimento por mais duas vezes, até aparecer a tela abaixo:



Cuidados ao cadastratar:

ATENÇÃO

- Orientar o correto posicionamento do dedo.
- Fazer a limpeza do sensor antes do cadastramento.
- Secar os dedos antes de colocá-los sobre o sensor.

Se quiser cadastrar mais uma impressão digital, basta selecionar o próximo dedo e seguir o procedimento a partir do **item 6.2.2**.

Todo cadastro é configurado inicialmente como **Digital de Acesso** (**bolinha azul**).

ATENÇÃO

- É recomendável cadastrar uma **Digital de Acesso** para cada mão, afim de facilitar a rotina de acesso.
- Por questões ergonômicas, evite cadastrar os dedos anelar e mínimo, pois é difícil posicioná-los corretamente sobre a célula biométrica do elevador.

Para recadastrar uma digital, é necessário primeiro apagar a digital anteriormente cadastrada, em seguida selecione a bolinha do dedo correspondente e clique no botão **APAGAR** ➔

. Feito isso, execute o procedimento a partir do **item 6.2.2**.

II) Opções pós-cadastro

As **bolinhas azul**, **verde** e **vermelha** são botões que devem ser utilizados para configurar o tipo de digital (**Acesso**, **Chave** e/ou **Alarme**).

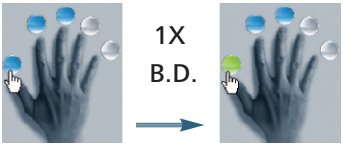
ATENÇÃO

Para o cadastramento da **Digital de Segurança** e/ou da **Digital Chave**, é necessário, primeiramente, realizar o cadastro de acesso de três digitais distintas. Ao término do cadastramento, os três dedos cadastrados estarão sinalizados com a **cor azul**.

Cadastro da Digital Chave

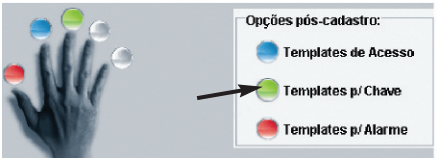
Existem duas maneiras para transformar o status de uma impressão **Digital de Acesso** para a **Digital Chave**:

- Escolha um dedo cadastrado, identificado com a **bolinha azul**. Clique uma vez com o **B.D.M.** (Botão Direito do Mouse) sobre a bolinha.



A partir daí, transforma-se a **Digital de Acesso** em **Digital Chave**, representada pela **cor verde**.

- Escolha um dedo cadastrado, identificado com a **bolinha azul**, efetue um clique no botão referente ao Template p/ Chave (**bolinha verde**), conforme figura abaixo:



A partir daí, transforma-se a **Digital de Acesso** em **Digital Chave**, representada pela **cor verde**.

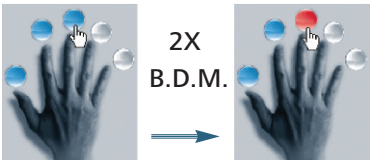
ATENÇÃO

Para que seja possível a utilização da **Digital Chave**, é imprescindível que, na tabela de acesso, um andar em pelo menos um elevador tenha sido configurado como **Andar Chave** - ver procedimento **Seleção do Andar Chave** (ver página 17).

Cadastro da Digital de Alarme

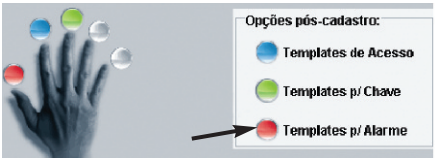
Existem duas maneiras para transformar o status de uma impressão **Digital de Acesso** para a **Digital Alarme**:

- Escolha um dedo cadastrado, identificado com a **bolinha azul**. Clique duas vezes com o **B.D.M.** (Botão Direito do Mouse) sobre a bolinha.



A partir daí, transforma-se a **Digital de Acesso** em **Digital de Alarme**, representada pela **cor vermelha**.

- Escolha um dedo cadastrado, identificado com a **bolinha azul**, efetue um clique no botão referente ao **Template para Alarme** (**bolinha vermelha**), conforme figura abaixo:

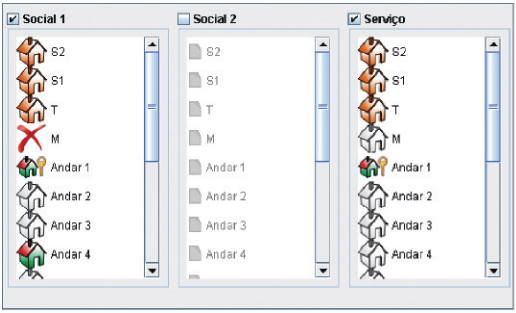


A partir daí, transforma-se a **Digital de Acesso** em **Digital de Alarme**, representada pela **cor vermelha**.

III) Configuração do acesso para biometria

Para cada usuário cadastrado com biometria, é necessário habilitar os elevadores e seus respecitvos andares autorizados.

Selecione o elevador a ser habilitado ☑ **Social 1**.



Configure o acesso, conforme a legenda:

- → **Andar de acesso**.
- → **Andar chave**.
- → **Andar bloqueado**.
- → **Andar comum**, liberado a todos os usuários.
- → **Andar X**, pavimento sem acesso via elevador.

Biometria: Seleção de Andares de Acesso

São os andares que o usuário está autorizado a acessar em um determinado elevador. Poderão ser configurados para um **morador**, **visitante** ou **funcionário**.

Para configurá-los, execute o seguinte procedimento:

a) Habilite o elevador ☑ **Social 1** .

b) Selecione o andar.

c) Clique uma vez com o **B.D.M.** (Botão Direito do Mouse) sobre a "**Casinha**" referente ao andar selecionado. A mudança de cor da figura da casinha ➔ confirma a nova configuração.

ATENÇÃO

O "**Andar de Acesso**" para Biometria deverá ser configurado por elevador na aba **Biometria**.

Biometria: Seleção do Andar Chave

É o andar que o usuário poderá ativar ou desativar a restrição de acesso, ou seja, liberar ou bloquear o acesso ao andar por meio da "**Digital Chave**". Poderá ser configurado apenas pelo usuário tipo "**Morador**".

Para configurá-lo, execute o seguinte procedimento:

a) Habilite o elevador ☑ **Social 1** .

b) Selecione o andar.

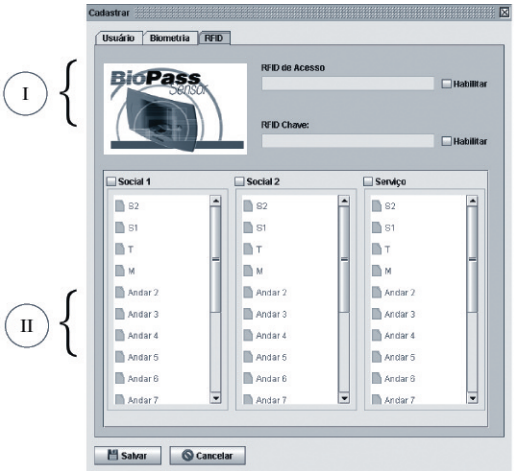
c) Clique duas vezes com o **B.D.M.** (Botão Direito do Mouse) sobre a "**Casinha**" referente ao andar selecionado. A mudança da figura da casinha ➔ , confirma a nova configuração.

ATENÇÃO

- O "**Andar Chave**" para Biometria deverá ser configurado por elevador na aba Biometria.
- É permitido a configuração de apenas um "**Andar Chave**" por elevador.

6.2.3. RFID: Cadastro do Cartão e Configurações de Acesso

A aba "**RFID**" é destinada ao cadastro do cartão **BioPass Sensor** e da configuração de acesso para uso do cartão:



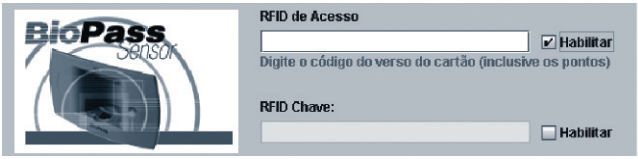
I) Cadastro do cartão RFID

II) Configuração do acesso RFID

I) Cadastro do Cartão RFID

Para cada usuário, é possível associar o cartão de proximidade do tipo **RFID**. Este cartão poderá ser habilitado como um **Cartão de Acesso** ou como um **Cartão Chave**, conforme procedimento a seguir:

a) Selecione a característica "**RFID de Acesso**" ou "**RFID Chave**", habiltando o campo de registro do número do cartão.



b) Digite o código gravado na parte inferior, à direita, no verso do cartão **BioPass Sensor** (inclusive os pontos), no campo referente ao **RFID de Acesso**, conforme ilustrado na figura abaixo:

ATENÇÃO

- Para cadastrar o **Cartão RFID Chave**, basta habilitar o campo referente ao "**RFID Chave**" e executar o procedimento acima.
- Somente usuários tipo "**Morador**" poderão ter o "**RFID Chave**" cadastrado.

Nota:

- Caso tenha usuário que necessite utilizar o **Cartão de Acesso** e **Cartão Chave**, será necessário cadastrar 2 cartões **BioPass Sensor**, sendo 1 no campo habilitado para **RFID** e o segundo para o **RFID Chave**.

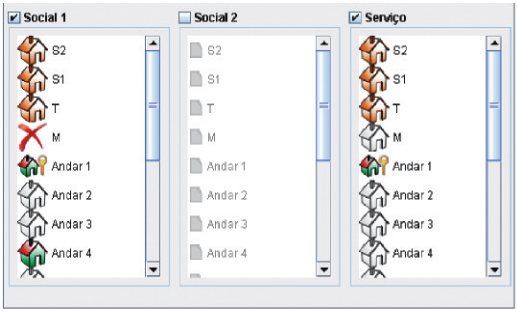
Alteração da numeração do cartão

Para alterar o número do cartão de acesso associado ao usuário, basta selecionar o campo **RFID de Acesso** ou **RFID Chave** e digitar o novo número do cartão de acesso.

II) Configuração do acesso para RFID

A configuração do acesso para **RFID** consiste em habilitar um ou mais andares em um determinado elevador.

Selecione o elevador a ser habilitado ☑ **Social 1** .



Configure o acesso, conforme a legenda:

- ➔ **Andar de acesso**.
- ➔ **Andar chave**.
- ➔ **Andar bloqueado**.
- ➔ **Andar comum**, liberado a todos os usuários.
- ➔ **Andar X**, pavimento sem acesso via elevador.

RFID: Seleção de Andares de Acesso

É o andar que o usuário está autorizado a acessar em um determinado elevador. Poderá ser utilizado por um **morador**, **visitante** ou **funcionário**.

Para configurá-los, execute o seguinte procedimento:

a) Habilite o elevador ☑ **Social 1** .

b) Selecione o andar.

c) Clique uma vez com o **B.D.M.** (Botão Direito do Mouse) sobre a "**Casinha**" referente ao andar selecionado. A mudança de cor da figura da casinha ➔ confirma a nova configuração.

ATENÇÃO

O "**Andar de Acesso**" para **RFID de Acesso** deverá ser configurado por elevador na aba **RFID**

RFID: Seleção do Andar Chave

É o andar que o usuário poderá ativar ou desativar o ***BioPass*** , ou seja, liberar ou bloquear, o andar por meio do **Cartão RFID Chave**. Poderá ser utilzado apenas pelo usuário tipo "**Morador**".

Para configurá-lo, execute o seguinte procedimento:

a) Habilite o elevador ☑ **Social 1** .

b) Selecione o andar.

c) Clique duas vezes com o **B.D.M.** (Botão Direito do Mouse) sobre a "**Casinha**" referente ao andar selecionado. A mudança da figura da casinha ➔ , confirma a nova configuração.

ATENÇÃO

- É permitido configurar apenas um "**Andar Chave**" por elevador.
- O "**Andar Chave**" para **RFID Chave** é configurado para todos os elevadores habilitados (flegados) na aba **RFID**, ou seja, a configuração efetuada em um determinado elevador, será válida para os demais elevadores habilitados ou que forem habilitados.

Concluído o cadastro do usuário, selecione o botão **Salvar** para gravar as informações na **Unidade Gerenciadora** e nas **Unidades Biométricas de Elevador**.

7. Possíveis problemas

Um usuário, mesmo que já cadastrado, poderá não ser reconhecido. Este problema é comum nas seguintes situações:

- Mau posicionamento do dedo, ou seja, o posicionamento do dedo na **Unidade de Leitura Biométrica** deverá ser similar ao posicionamento adotado na **Unidade Biométrica de Cadastramento**.
- Não estar cadastrado no respectivo elevador.
- Dia e/ou horário não permitido(s) para funcionário ou visitante.
- Sensor sujo.
- Cortes ou modificações significativas sobre a superfície do dedo cadastrado.
- Excesso de sudorese nas mãos.
- Célula biométrica danificada.
- **Cartão RFID** inválido.
- **Cartão RFID** não cadastrado.
- **Cartão RFID** danificado.

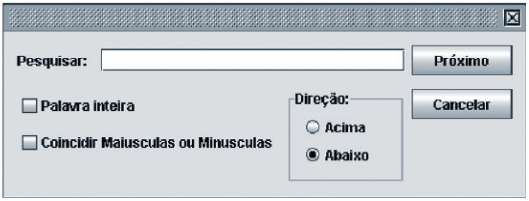
Se o usuário apresentar uma frequente rejeição de reconhecimento e não for devido a nenhuma destas razões, recomenda-se refazer o cadastramento ou substituir o cartão associado ao usuário.

8. Gerenciamento

8.1. Localizar usuário

A busca por um usuário ou o número de um cartão é facilitada selecionando o item "**Localizar**" no menu "**Usuário**" ou pelo atalho **< CTRL + F >** pressionando as teclas **CTRL** e **F** simultaneamente.

Para efetuar a pesquisa, digite o nome do usuário no campo "**Pesquisar**" em seguida selecione o botão "**Próximo**".

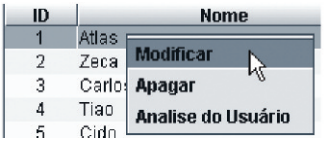


8.2. Modificar usuário

As propriedades de um usuário podem ser modificadas através das seguintes ações:

- No menu "**Usuários**", selecione o item "**Modificar**".

- No campo "**Usuários**", clique no usuário a ser modificado; em seguida, pressione o **B.D.M.** (Botão Direito do Mouse) e selecione o item "**Modificar**".



- No campo "**Usuários**", selecione o usuário a ser modificado e efetue um duplo clique sobre o nome.

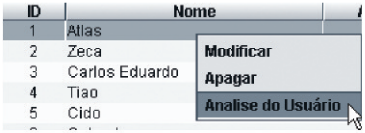
No **capítulo 6.2**, está o procedimento para cadastrar os dados básicos e perfil de acesso, biometria e cartão e suas respectivas configurações de acesso.

8.3. Análise do Usuário

É possível verificar em quais elevadores um determinado usuário está cadastrado.
Para isso, será necessário:

a) No campo de usuários cadastrados, selecione o usuário.
b) Clique com o **B.D.M.** (Botão Direito do Mouse) no usuário selecionado.
c) Selecione a função "**Análise do Usuário**".

Feito isso, o sistema irá verificar se o usuário está com a biometria e/ou cartão cadastrado no(s) elevador(es).

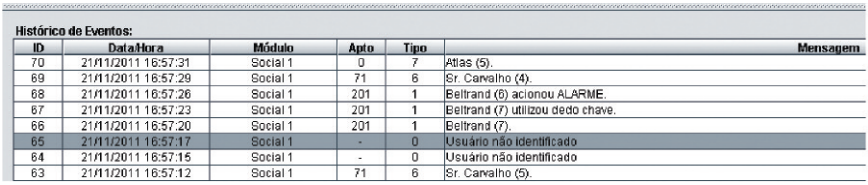


ATENÇÃO

As informações referentes ao **RFID** só são válidas para as **Unidades Biométrica de Elevador** com versão de *firmware* igual ou superio a 516a. Caso necessite saber a versão do *firmware*, contate o **Suporte** da Atlas Schindler.

8.4. Histórico de eventos

O ***BioPass*** tem a capacidade de armazenamento de um histórico de eventos da utilização do sistema.



Histórico de Eventos:

ID	Data/Hora	Módulo	Apto	Tipo	Mensagem
70	21/11/2011 16:57:31	Social 1	0	7	Atlas (5).
69	21/11/2011 16:57:29	Social 1	71	6	Sr. Carvalho (4).
68	21/11/2011 16:57:26	Social 1	201	1	Beltrand (6) acionou ALARME.
67	21/11/2011 16:57:23	Social 1	201	1	Beltrand (7) utilizou dedo chave.
66	21/11/2011 16:57:20	Social 1	201	1	Beltrand (7).
65	21/11/2011 16:57:17	Social 1	-	0	Usuário não identificado
64	21/11/2011 16:57:15	Social 1	-	0	Usuário não identificado
63	21/11/2011 16:57:12	Social 1	71	6	Sr. Carvalho (5).

No **Histórico de Eventos**, são registrados o dia e a hora para:
- Status de operação do sistema.
- Utilização dos elevadores pelos usuários.
- Cadastramento e exclusão de usuários.
- Modificações nas propriedades dos usuários.

Todos os eventos registrados são memorizados e arquivados na **Unidade Gerenciadora**. Ao exportá-los, o sistema converte os dados para o formato "**.csv**", permitindo a transferência através da porta de comunicação **USB**, para análise e edição externa. Para a transferência, pode ser utilizado um dispositivo tipo "**Pen Drive**" (dispositivo não fornecido com o equipamento).

A exportação do "**Histórico de Eventos**" poderá ser automática ou manual, em ambas as opções, o sistema salvará o arquivo com extensão **.csv** no diretório "**C:\Java\BioPass**".

Para evitar sobrescrever os Históricos de Eventos exportados anteriormente, o sistema define a denominação dos arquivos, obedecendo a seguinte regra "**aaaa-mm-dd_hh-mm-ss_Nome do Condomínio**", sendo:

aaaa = ano
mm = mês
dd = dia
hh = hora
mm = minuto
ss = segundo

Exportação automática do Histórico de Eventos

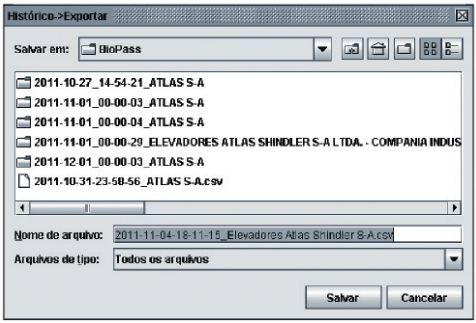
A exportação automática do **Histórico de Eventos** acontece quando:

- Atingir **10.000 eventos** no sistema.
- Todo **dia 1º** de cada mês às **00h00**.

Exportação manual do Histórico de Eventos

Para exportar manualmente o **Histórico de Eventos**, execute o seguinte procedimento:

a) No menu "**Sistema**", acesse o item "**Histórico**".
b) Selecione a função "**Exportar**". O sistema abrirá uma janela com o nome do arquivo "**.csv**".
c) Clique no botão "**Salvar**". Feito isso, o sistema salvará o **Histórico de Eventos** no diretório "**C:\Java\BioPass**".



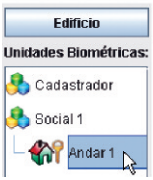
9. Funções avançadas

9.1. Andares liberados pelo usuário

O sistema **BioPass** permite através da 2ª impressão digital, denominada **Digital Chave**, ou do cartão de acesso, denominado **RFID Chave**, liberar ou restringir o acesso a um determinado andar.

A **Digital Chave** ou o **RFID Chave** constitui-se em uma ferramenta importante na flexibilização do acesso em eventos como festas, mudanças, reformas etc. Seu conceito de funcionamento é simples, similar a uma chave. Quando acionado, libera o acesso ao pavimento associado. Acionado novamente, restringe (bloqueia) o acesso ao pavimento anteriormente liberado.

Tendo em vista a importância da **Digital Chave** na segurança do sistema, toda vez que a **Digital Chave** ou o **RFID Chave** for utilizada, será sinalizado na tela da **Unidade Gerenciadora** qual elevador e andar tiveram seu acesso **Liberado**.



Toda vez que aparecer a figura da casinha com a denominação do andar, significa que este andar foi liberado por meio da "**Digital Chave**" ou "**RFID Chave**", ou seja, a restrição de acesso foi desabilitada para este andar.

9.2. Bloqueio do andar liberado pelo usuário

Existem 2 formas de reativar a restrição de acesso nos andares que foram liberados por meio da "**Digital Chave**" e/ou "**RFID Chave**":

– Bloqueio do andar pelo usuário

Para bloquear novamente o andar liberado pela **Digital** ou **RFID Chave**, basta o morador utilizar novamente a "**Digital Chave**" ou o "**RFID Chave**".

– Bloqueio do andar pelo operador

Face a possibilidade de esquecimento pelos usuários do andar com o status liberado, foi implementado no gerenciador a função de se reestabelecer o status de restrição de acesso. Basta executar o seguinte procedimento:

1) Na estrutura de andares liberados, selecione o andar a ser bloqueado.
2) Pressione o **B.D.M.** (Botão Direito do Mouse) sobre o andar selecionado e clique em **Remover Andar**.
3) O andar liberado pela **Digital Chave** ou **RFID Chave** novamente foi bloqueado.

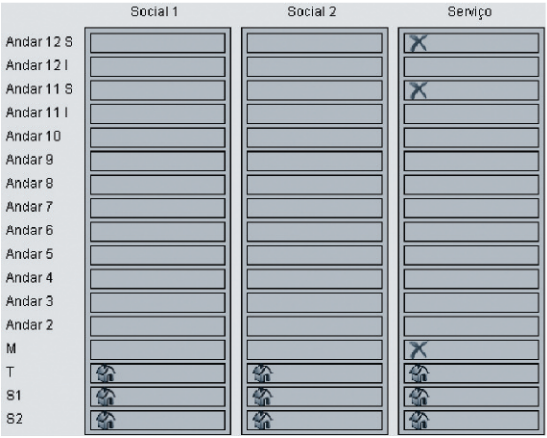
9.3. Andares comuns

Andares comuns são todos os andares, definidos pelo edifício, que terão seu acesso liberado a todos os usuários, independente do acesso biométrico.

Constituem normalmente andares comuns como: térreo, salão de festas, salão de ginástica etc. A configuração de andares comuns somente está disponível para os usuários com o nível **Suporte** (Técnicos Atlas Schindler).

9.4. Andar X

Denomina-se como "**Andar X**" o andar que, por algum motivo, determinado o elevador não para ou não tem acesso.



ATENÇÃO

A configuração de andares **X** somente está disponível para os usuários com o nível **Suporte** (Tecnicos Atlas Schindler).

9.5. Capturar imagem

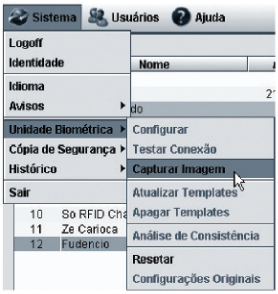
A captura de imagem é um recurso avançado para a verificação da qualidade da impressão digital de cada usuário e para a análise das condições de uso das células biométricas.

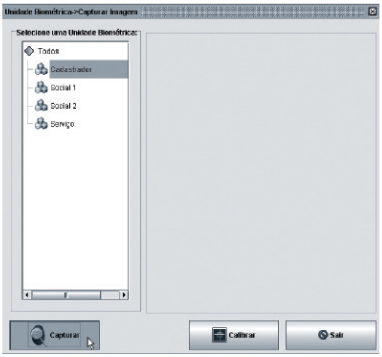
ATENÇÃO

Esta função está disponível somente nos perfis **Suporte** e **Administrador**.

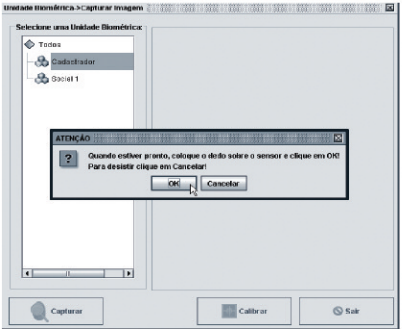
Para acessar esta função, execute o procedimento a seguir:

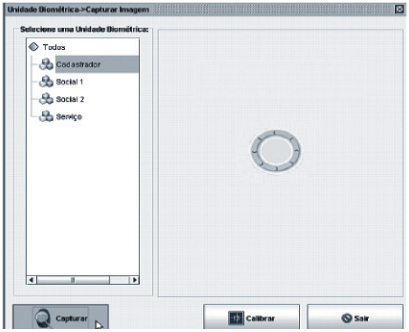
a) No menu "**Sistema**", acesse o item "**Unidade Biométrica**".
b) Selecione a função "**Capturar Imagem**".
c) Escolha uma "**Unidade Biométrica**" a ser utilizada.
d) Clique no botão "**Capturar**".



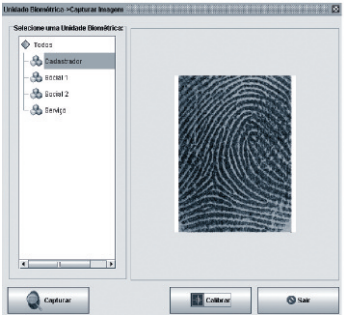


e) Posicione a "**1ª falange**" do dedo sobre a "**parte sobressalente**" da célula biométrica. Clique no botão "**OK**", permanecendo com o dedo sobre a célula até que o **led verde** na leitora se apague.





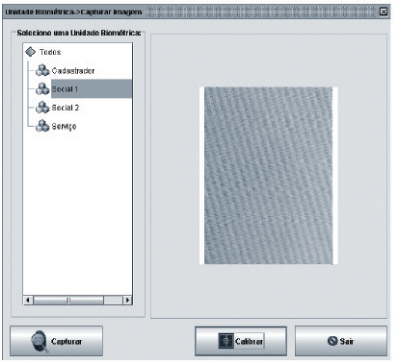
f) O sistema exibirá a imagem da digital capturada.



ATENÇÃO

É válido ressaltar que a função "**Capturar Imagem**" não grava as informações.

O procedimento de Captura de Imagem permite também verificar o estado da célula biométrica, quanto a risco, sujeira etc. Neste caso, refaça o procedimento de "**Capturar a Imagem**", porém não coloque o dedo sobre a célula biométrica.



Calibrar

O botão "**Calibrar**" tem como função alinhar o contraste entre o **ID Module** e **FingerTip**. Siga o procedimento abaixo para executar a função "**Calibrar**"

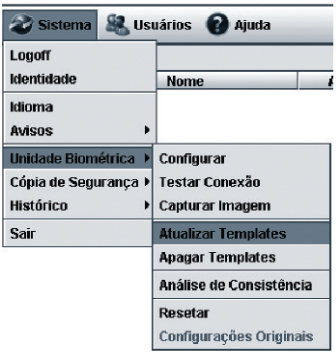
a) Selecione o "**Módulo Biométrico**".
b) Clique no botão "**Calibrar**".

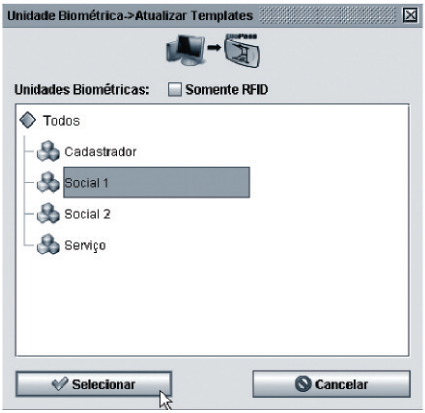
Neste momento o sistema alinhará o contraste entre o **ID Module** e o **FingerTip**.

9.6. Atualizar Templates

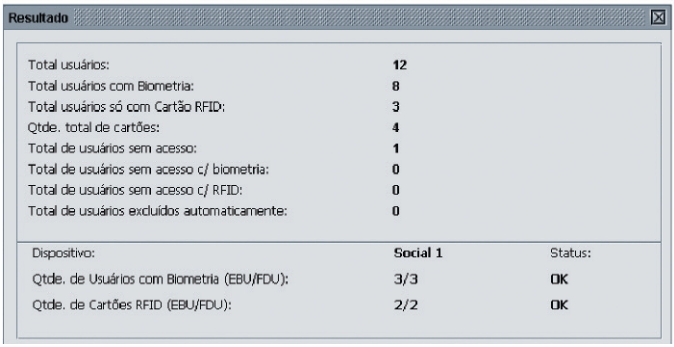
A função "**Atualizar Templates**" envia para o módulo biométrico os templates (cadastros) dos usuários. Esta função está disponível para os níveis **Suporte** e **Administrador**.

Siga o procedimento abaixo para executar a função "**Atualizar Templates**":
a) No menu "**Sistema**", acesse o item "**Unidade Biométrica**".
b) Selecione a função "**Atualizar Templates**".
c) Selecione o "**Módulo Biométrico**".
d) Clique no botão "**Selecionar**". Feito isso, o sistema inicia o processo de atualização de templates.





Ao término da atualização, o sistema apresentará a análise de consistência do(s) módulo(s) biométrico atualizado.


Resultado
Total usuários: 12
Total usuários com Biometria: 8
Total usuários só com Cartão RFID: 3
Qtde. total de cartões: 4
Total de usuários sem acesso: 1
Total de usuários sem acesso c/ biometria: 0
Total de usuários sem acesso c/ RFID: 0
Total de usuários excluídos automaticamente: 0
Dispositivo: Social 1 Status:
Qtde. de Usuários com Biometria (EBU/FDU): 3/3 OK
Qtde. de Cartões RFID (EBU/FDU): 2/2 OK

ATENÇÃO

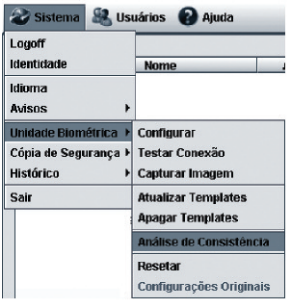
Se na coluna **Status** aparecer alguma falha, conforme ilustrado na figura abaixo, significa que houve algum problema no envio dos pacotes. Assim execute novamente a função "**Atualizar Templates**".

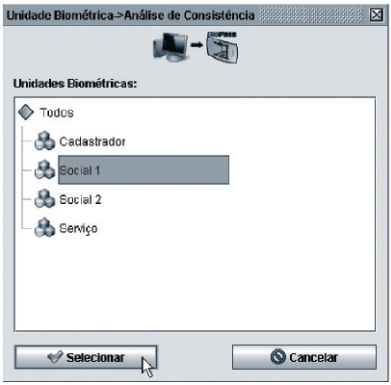
Dispositivo:	Social 1	Status
Qtde. de Usuários com Biometria (EBU/FDU):	40/44	Falha
Qtde. de Usuários com RFID (EBU/FDU):	1/4	Falha

9.7. Análise de Consistência

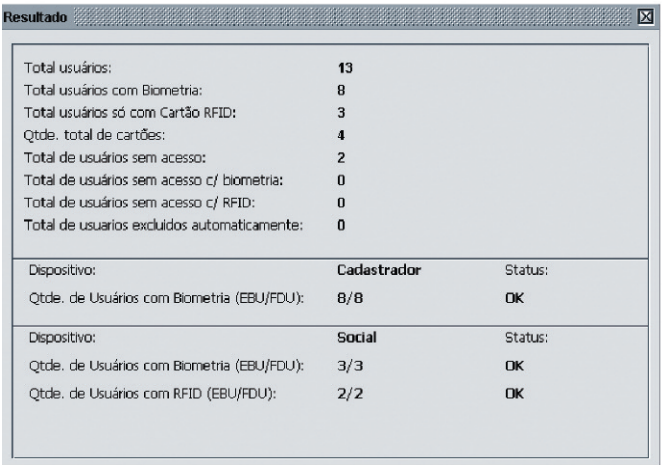
A função "**Análise de Consistência**" tem como objetivo analisar se os módulos biométricos estão atualizados com os **Templates** (cadastros) e **RFID**.

Siga o procedimento abaixo para executar a função "**Análise de Consistência**".
a) No menu "**Sistema**", acesse o item "**Unidade Biométrica**".
b) Selecione a função "**Análise de Consistência**".
c) Selecione o "**Módulo Biométrico**" e clique no botão "**Selecionar**".





Em seguida aparecerá o resultado da **Análise de Consistência**:


Resultado
Total usuários: 13
Total usuários com Biometria: 8
Total usuários só com Cartão RFID: 3
Qtde. total de cartões: 4
Total de usuários sem acesso: 2
Total de usuários sem acesso c/ biometria: 0
Total de usuários sem acesso c/ RFID: 0
Total de usuarios excluidos automaticamente: 0
Dispositivo: Cadastrador Status:
Qtde. de Usuários com Biometria (EBU/FDU): 8/8 OK
Dispositivo: Social Status:
Qtde. de Usuários com Biometria (EBU/FDU): 3/3 OK
Qtde. de Usuários com RFID (EBU/FDU): 2/2 OK

ATENÇÃO

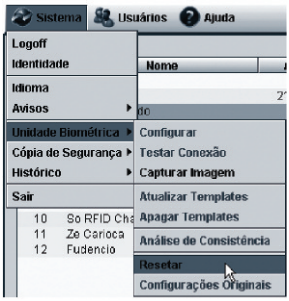
Se na coluna **Status** aparecer alguma falha, conforme ilustrado na figura abaixo, significa que houve algum problema no envio dos pacotes. Assim, execute novamente a função "**Atualizar Templates**".

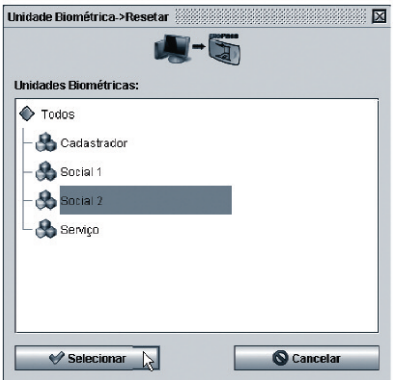
Dispositivo:	**Social 1**	Status
Qtde. de Usuários com Biometria (EBU/FDU):	**40/44**	**Falha**
Qtde. de Usuários com RFID (EBU/FDU):	**1/4**	**Falha**

9.8. Reinicialização: Resetar

Este comando permite que as **Unidades Biométricas de Elevador** e de **Portaria** sejam reinicializadas manualmente, quando uma situação indevida impeça o seu funcionamento.

Para acessar esta função, execute o procedimento a seguir:
a) No menu "**Sistema**", acesse o item "**Unidade Biométrica**".
b) Selecione a função "**Resetar**".
c) Escolha o "**Módulo Biométrico**" a ser resetado e em seguida clique no botão "**Selecionar**".





ATENÇÃO

Esta função somente está disponível para os níveis de **Administrador** e **Suporte**.

9.9. Cópia de Segurança

A função "**Cópia de Segurança**" é utilizada para efetuar o backup do sistema, ou seja, salvar os registros de usuários contidos na pasta "**Templates**" e os arquivos "**biopass.db**" e **log.db**. A Cópia de Segurança poderá ser gerada: automaticamente e/ou manualmente.

Em ambas as opções, toda vez que a função **Cópia de Segurança** for executada, o sistema criará uma pasta no diretório "**C:\Java\BioPass**". Para evitar sobrescrever as **Cópias de Segurança** anteriores, a denominação desta pasta obedecerá a seguinte regra: "**aaaa-mm-dd_hh-mm-ss_Nome do Condomínio**", sendo:

aaaa = ano
mm = mês
dd = dia
hh = hora
mm = minuto
ss = segundo

– Gerar Cópia de Segurança automaticamente

Todo **1º dia** de cada mês às **00h00**, o **BioPassJava** irá gerar automaticamente a "**Cópia de Segurança**" do sistema.

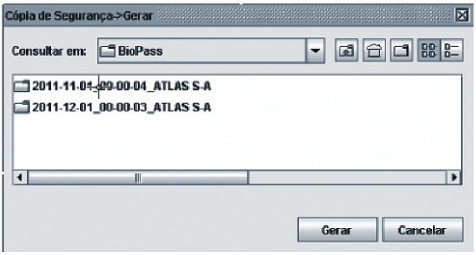
– Gerar Cópia de Segurança manualmente

Para gerar manualmente a "**Cópia de Segurança**" do sistema, execute o seguinte procedimento:

a) No menu "**Sistema**", acesse o item "**Cópia de Segurança**".

b) Selecione a função "**Gerar**".

c) Na janela seguinte, selecione o botão "**Gerar**".



Feito isso, o sistema executará o **backup** do sistema.

– Restaurar Cópia de Segurança

O sistema permite restaurar a cópia de segurança apenas da pasta **Templates** e do arquivo **biopass.db**. Para isso, execute o seguinte procedimento:

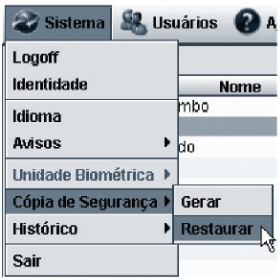
a) No menu "**Sistema**", acesse o item "**Cópia de Segurança**".

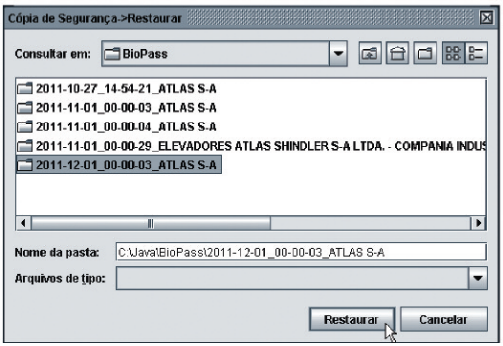
b) Selecione a função "**Restaurar**".

c) Verifique a data e horário das pastas.

d) Selecione a pasta.

e) Clique no botão "**Restaurar**".





9.10. Status do usuário

Através do campo de usuários cadastrados é possível ter um resumo do cadastro dos usuários, como: nome, apartamento, tipo de acesso, horário de acesso, elevadores, número e tipo de cartões de acesso associados.

Os usuários marcados com uma faixa na **cor vermelha**, sinaliza que estes usuários foram excluídos da **Unidade Biométrica** de **Elevador** por meio da função **Tempo Limite de Uso**, conforme figura abaixo:

ID	Nome	Apto	Tipo	Horário de Acesso	Elevador	RFID de Acesso	RFID Chave
20	Tatiana de Souza	50	Visitante Fixo	--	1	--	--
21	Helena	190	Visitante	08:>1 - 23:57	1	--	--
22	Roberta	9	Visitante Fixo	--	2	--	--

Os usuários marcados com uma faixa na **cor amarela** sinaliza que estes usuários estão sem acesso.

ID	Nome	Apto	Tipo	Horário de Acesso	Elevador	RFID de Acesso	RFID Chave
16	Inacio Monteiro	230	Funcionário	00:00 - 23:59	1,2,3,4	--	--
17	Silvia Bruna	9	Visitante Fixo	--	--	--	--
18	Carolina Lara	9	Visitante Fixo	--	2	--	--

Define-se como usuário sem acesso:

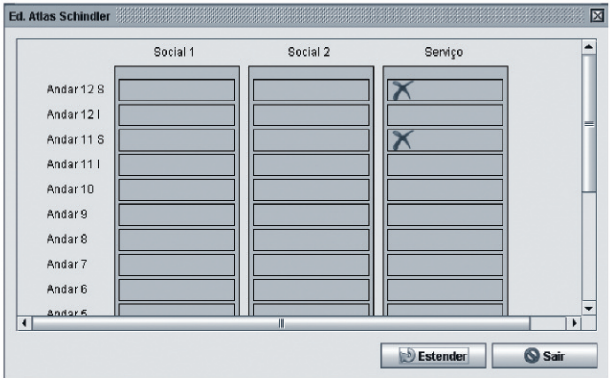
- O usuário que não tem biometria e cartão cadastrados.
- Usuário somente com biometria cadastrada, mas não foi selecionado nenhum elevador na **aba Biometria**, ou seja, não tem acesso aos elevadores.
- Usuário somente com cartão de acesso **RFID** e/ou **RFID Chave**, mas não foi selecionado nenhum elevador na **aba RFID**, ou seja, não tem acesso aos elevadores.
- Usuários com **Biometria** e/ou cartão de acesso **RFID** e **RFID Chave** cadastrados, mas não foi selecionado nenhum elevador nas **abas Biometria** e **RFID**, ou seja, não tem acesso aos elevadores.

9.11. Edifício

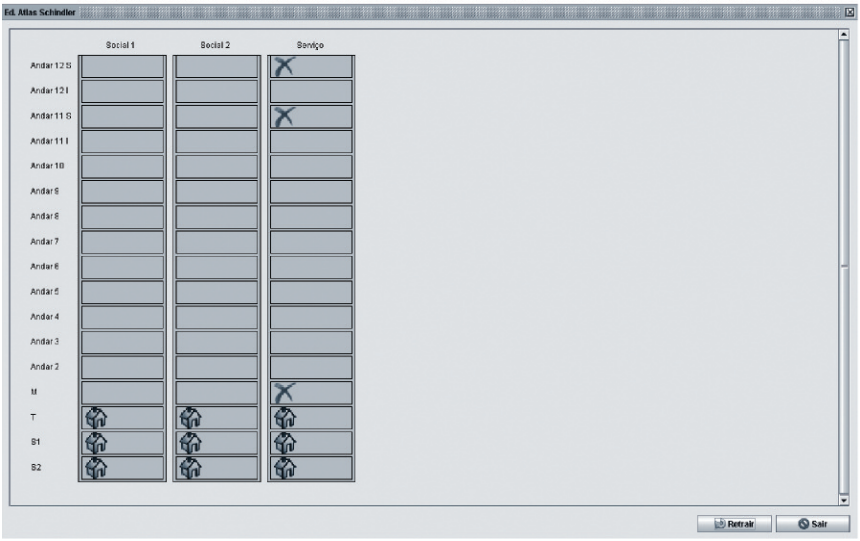
A função "**Edifício**" é utilizada para obter uma visão geral do condomínio, sendo apresentadas as seguintes informações:

- A quantidade de paradas por elevador.
- A configuração dos andares "**X**" por elevador.
- Os andares liberados pela **Digital Chave** e/ou cartão **RFID Chave** por elevador.

Para acessar esta função, clique no botão **Edifício**, localizado sobre a estrutura de andares liberados. A seguinte informação será apresentada com uma visão geral do condomínio:



O botão **Estender** permite uma visão panorâmica do condomínio.



9.12. Habilitar Aviso de Alarme

O aviso de alarme tem como objetivo apresentar a mensagem de alerta, na tela do **Gerenciador**, quando a digital de alarme for utilizada. As demais ações permanecem as mesmas: acionamento do sinal para o sistema de segurança e registro na lista do Histórico de Eventos.

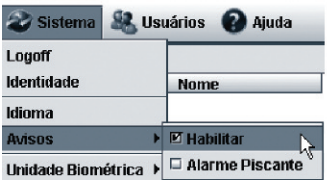
O aviso de alarme poderá ser de forma discreta ou piscante, conforme descrito abaixo:

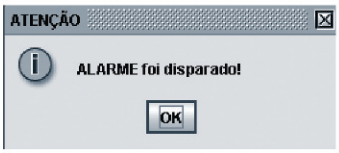
– Alarme Discreto

Para configurar o "**Alarme Discreto**", execute o procedimento abaixo:

a) No menu "**Sistema**", item "**Avisos**".

b) Selecione "**Habilitar**".





– Alarme Piscante

Para configurar o "**Alarme Piscante**", execute o procedimento abaixo:

a) No menu "**Sistema**", item "**Avisos**".

b) Selecione "**Alarme Piscante**".

9.13. Mudança de Idioma

Disponível no menu "**Sistema**", item "**Idioma**", permite que o sistema gerenciador se adapte ao idioma onde o ***BioPass*** está sendo instalado. Idiomas disponíveis: **Português**, **Espanhol** e **Inglês**.

10. Advertência

Como todo sistema eletrônico destinado ao uso público, ou restrito, seja ele para controle de acesso ou não, regras para a sua adequada utilização são necessárias:

Restrição de uso

Eletricidade estática - Ambientes demasiadamente secos podem intensificar a geração de eletricidade estática podendo danificar ou reduzir a vida útil das células biométricas.

Umidade - Dedos molhados ou excessivamente úmidos podem impedir a leitura das características biométricas. Usuários com sudorese deverão enxugar as mãos antes de executar o reconhecimento.

Sujeira - Pó excessivo depositado sobre a célula biométrica, dedos sujos de gordura (fritura, chocolates ou cremes para as mãos) podem causar dificuldade no reconhecimento biométrico. Neste caso do pó, a abrasividade pelo atrito pode reduzir a vida útil da célula biométrica.

O mesmo se aplica para o cartão de proximidade, que não é reconhecido quando posicionado afastado da leitura ou longe da região identificada com o símbolo .
Posicionamento - Posicionamento inadequado ou displicente também pode causar erro na leitura e, consequentemente, o não reconhecimento biométrico.

Limpeza - Deverão ser seguidas as orientações contidas no capítulo **Cuidados com o equipamento**.

ATENÇÃO

Pessoas com ausência de digitais, mãos extremamente secas, idosos ou crianças com dedos pequenos podem sentir dificuldades no cadastramento e impossibilitar a leitura e operação do elevador. Neste caso, recomenda-se que estejam acompanhadas durante a viagem de acesso aos pavimentos.

Concept

Impresso em 2012

51947261

003760 V4

Elevadores Atlas Schindler S.A.
Avenida do Estado, 6116 - Cambuci
CEP 01516-900 - São Paulo - SP

SAC 0800 055 1918
www.atlas.schindler.com